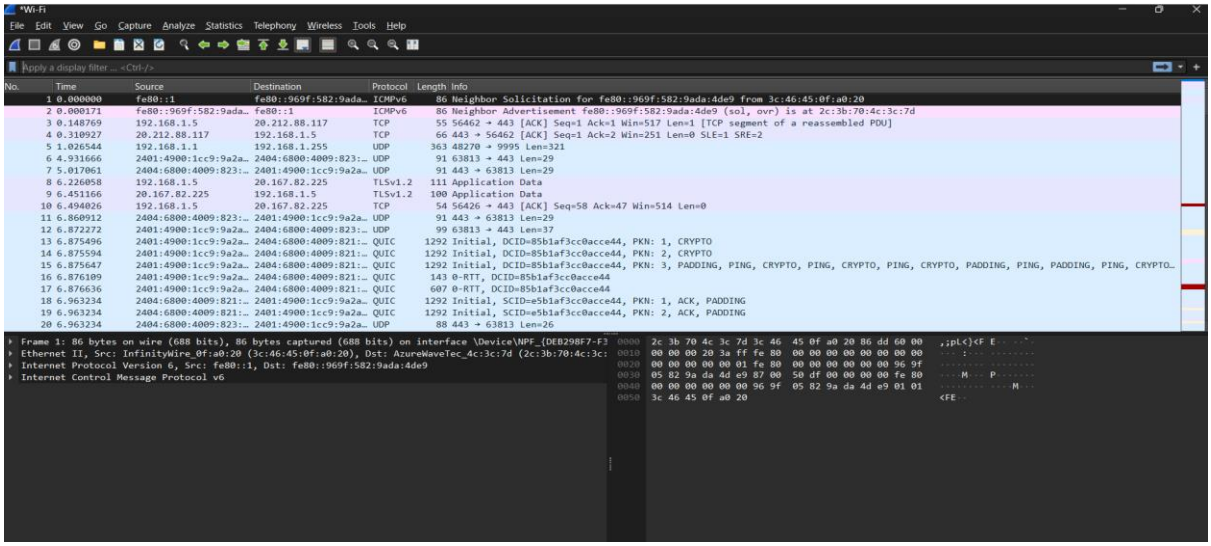
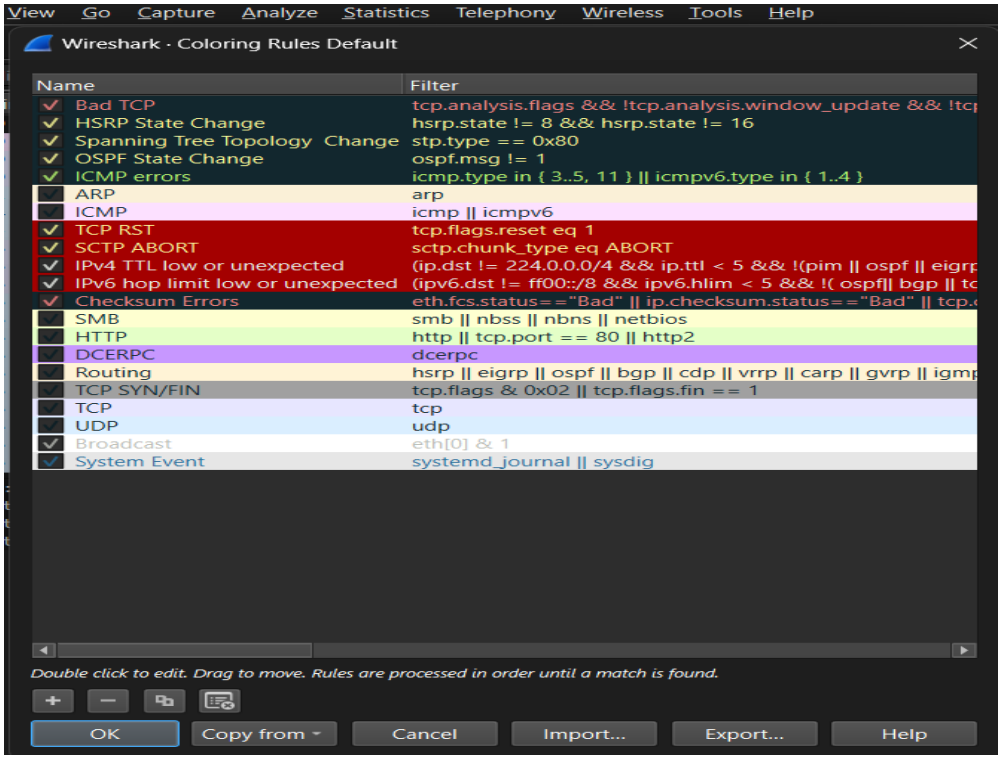
Practical -5

Experiments on Packet capture tool: Wireshark

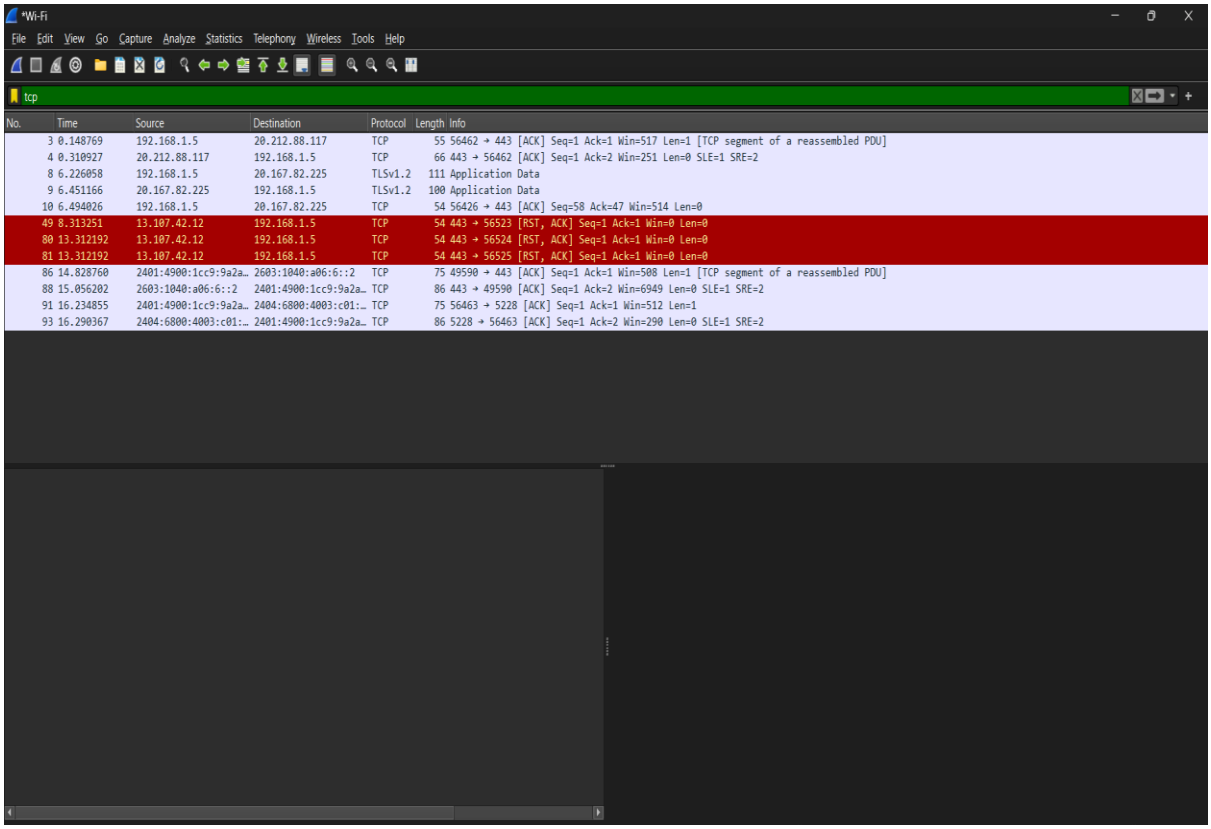
Capturing Packets



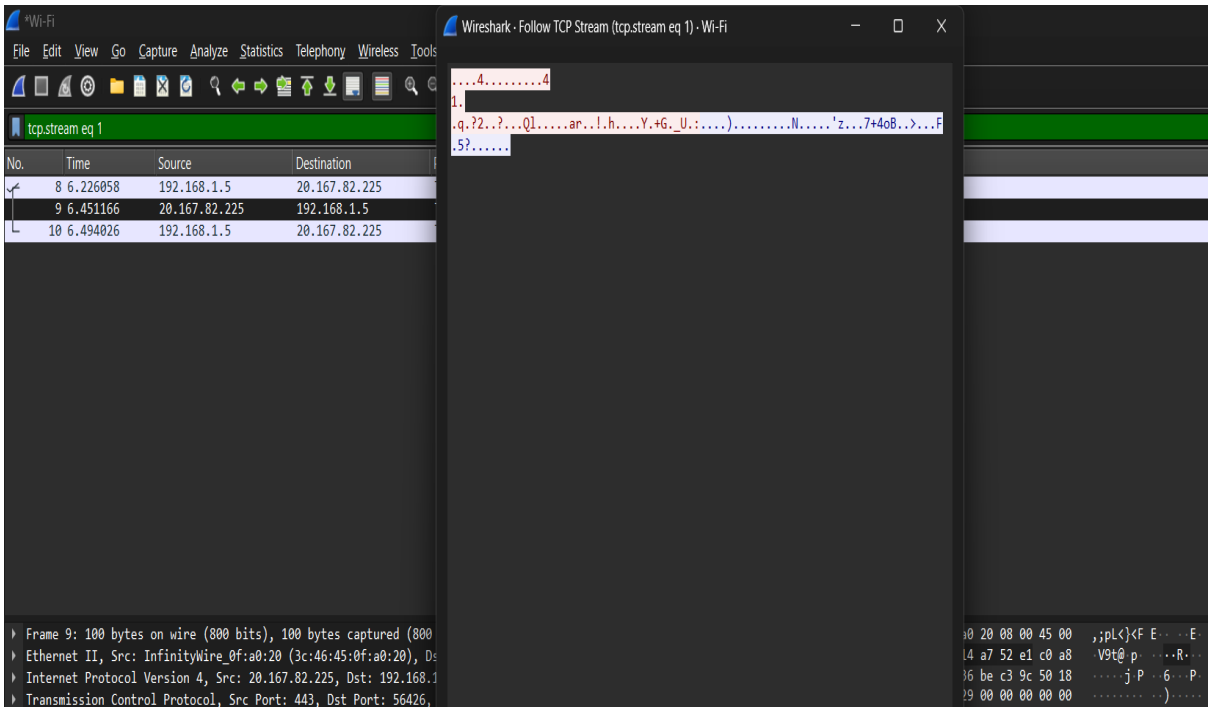
Color Coding



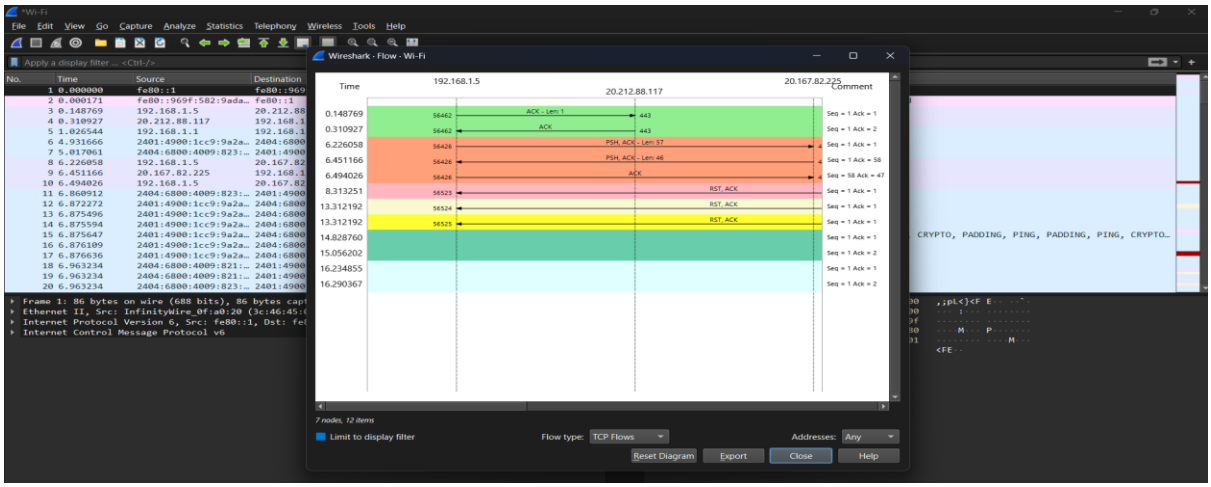
Filtering Packets



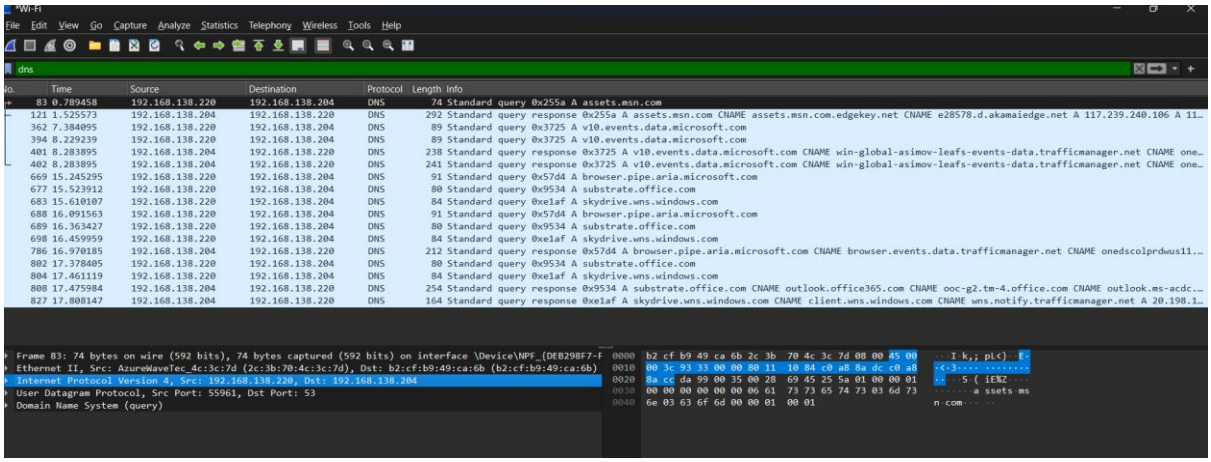
TCP Stream



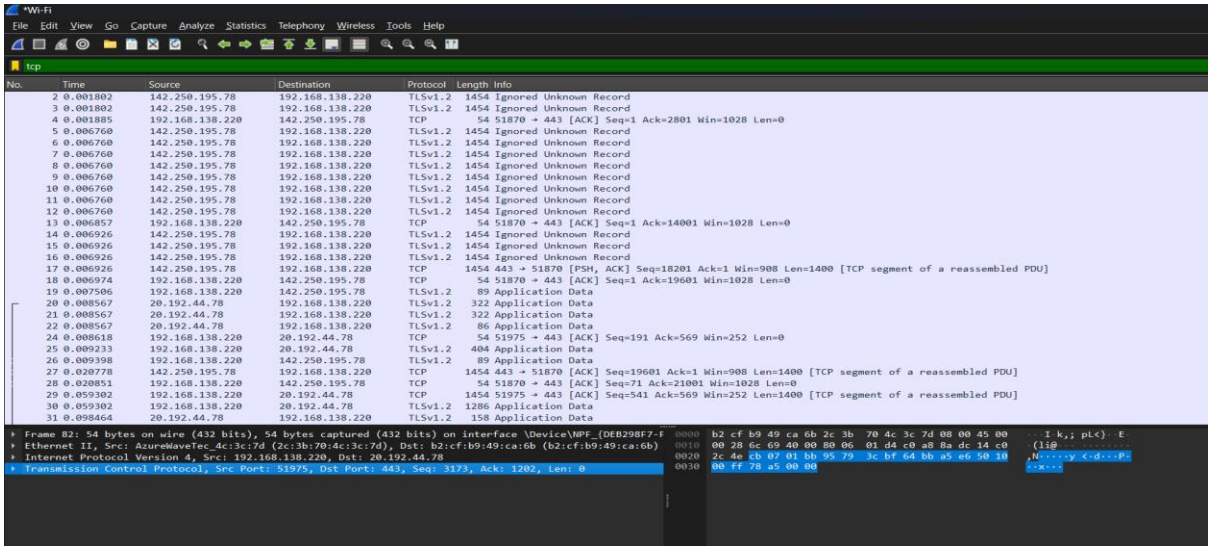
Flow Graph:



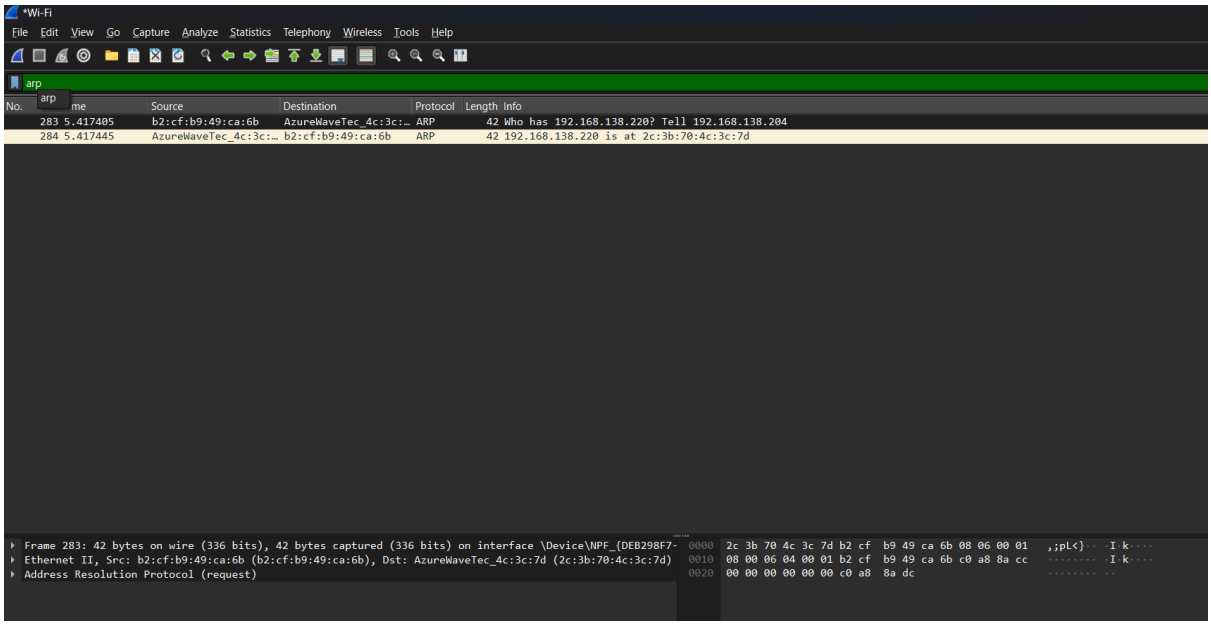
DNS:



TCP



ARP


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
arp
No. Time Source Destination Protocol Length Info
283 5.417405 b2:cf:b9:49:ca:6b AzureWaveTec_4c:3c:… ARP 42 Who has 192.168.138.220? Tell 192.168.138.204
284 5.417445 AzureWaveTec_4c:3c:… b2:cf:b9:49:ca:6b ARP 42 192.168.138.220 is at 2c:3b:70:4c:3c:7d
Frame 283: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{DEB298F7-
Ethernet II, Src: b2:cf:b9:49:ca:6b (b2:cf:b9:49:ca:6b), Dst: AzureWaveTec_4c:3c:7d (2c:3b:70:4c:3c:7d)
Address Resolution Protocol (request)
0000 2c 3b 70 4c 3c 7d b2 cf b9 49 ca 6b 08 06 00 01
0010 08 00 06 04 00 01 b2 cf b9 49 ca 6b c0 a8 8a cc
0020 00 00 00 00 00 00 c0 a8 8a dc